ABSTRACT OF THE DISCLOSURE

A signature calculation system includes: a mobile agent for calculating a digital signature of the owner of the mobile agent; a base host of the mobile agent from which the mobile agent starts moving in a network; and remote hosts in the network which can be visited by the mobile agent. In the base host in which the mobile agent is activated, a secret key #0 of the owner of the mobile agent is partitioned and distributed into cipher texts (partial signature auxiliary data) that can be restored only when calculations by use of secret keys of k remote hosts are executed, and data including the cipher texts are stored in the mobile agent. A remote host visited by the mobile agent arbitrarily presents signature target data. If the mobile agent determined to write a digital signature for the signature target data, the mobile agent stores the signature target data and moves to the next remote host. Thereafter, each remote host visited by the mobile agent calculates a partial signature by use of the data stored in the mobile agent and a secret key of the remote host. After the mobile agent visited k remote hosts since the presentation of the signature target data, the mobile agent returns to the remote host that presented the signature target data, at which the digital signature for the signature target data by use of the secret key of the owner of the mobile agent is obtained from the partial signatures calculated by the k remote hosts.